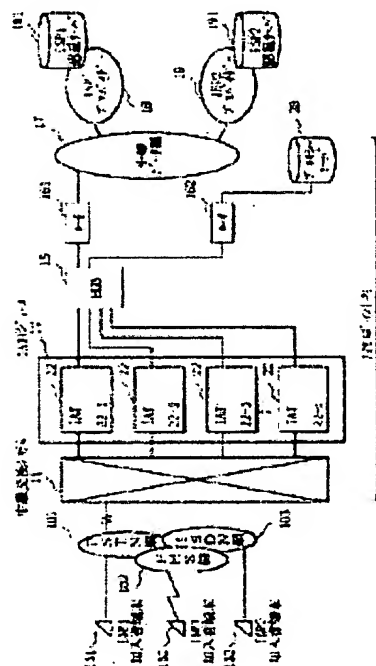


(11)Publication number : 2001-237892  
(43)Date of publication of application : 31.08.2001

(21)Application number : 2000-049130      (71)Applicant : NEC CORP  
(22)Date of filing :            25.02.2000      (72)Inventor : NAKAMURA MASAKAZU

**SOLUTION:** When an outgoing subscriber terminal 131 dials a dialup access number, a relay exchange system 11 translates the dialup access number and the translated number reaches an IAT 22. After PPP termination, a corresponding ISP is recognized from a user same (domain name) of the outgoing subscriber terminal 131 and a password, and an address of an authentication server of the ISP acquired. After the end of authentication, an IP address of the outgoing subscriber terminal, an IP address of an access router and an IP address of a DNS server are acquired from user data of each ISP stored in a proxy server 28 to attain access to the ISP. Thus, using one dialup number can access a plurality of providers.



\* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

CLAIMS

---

[Claim(s)]

[Claim 1]In an Internet access method using an access server provided with the Internet access trunk which remote accesses an Internet Service Provider, An Internet access method using an access server, wherein said Internet access trunk has an accessing means which accesses two or more Internet Service Providers by a unified dialup number.

[Claim 2]Said accessing means, It installs in an access point. A certain proxy server. Use and an Internet Service Provider's service. An Internet access method using the access server according to claim 1 discriminating said Internet access service provider from a user name (domain name) of \*\*\*\*\* and a password which have won popularity.

[Claim 3]Said accessing means, It installs in an access point. A certain proxy server. Use and an Internet Service Provider's service. An Internet access method using a claim 1 written access server discriminating an authentication server of an Internet Service Provider who checks user authentication from a user name (domain name) of \*\*\*\*\* and a password which have won popularity.

[Claim 4]Said accessing means, An IP address of a router connected to said Internet Service Provider from system data which carried out internal organs to said proxy server, an IP address of an applicable Internet Service Provider's DNS server, and an IP address of \*. Acquiring claims 1 and 2 or an Internet access method using an access server given in three.

[Claim 5]It is an Internet accessing method using an access server provided with the Internet access trunk which remote accesses an Internet Service Provider, An Internet accessing method using an access server, wherein said Internet access trunk accesses two or more Internet Service Providers by a unified dialup number.

[Claim 6]It is an Internet accessing method using an access server provided with the Internet access trunk which remote accesses an Internet Service Provider, A proxy server is used for said Internet access trunk, If an IP address of an authentication server which checks user authentication from a domain name to an authentication demand sent from \*\*\*\*\* is acquired, said authentication server is accessed, attestation is performed and attestation is successful, If an attestation Acknowledgement is replied to the aforementioned from subscriber terminal, and an IP address assignment request comes from said subscriber terminal after replying an attestation Acknowledgement to the aforementioned from subscriber terminal, An Internet accessing method using an access server acquiring an IP address assigned to a subscriber terminal and an IP address of an Internet Service Provider's DNS, and assigning said Internet Service Provider's IP address.

---

[Translation done.]

**\* NOTICES \***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

**DETAILED DESCRIPTION**

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention about the method and method of an Internet access system, It is related with the Internet access method and method using the share access server in a function of a remote access server of the relay exchange which has the Internet access trunk (it is called Internet Access Trunk:IAT) especially, or a member exchange system.

[0002]

[Description of the Prior Art]Generally one or more dialup numbers are assigned to one ISP (Internet Service Provider: abbreviated may be carried out and it may be called a provider an Internet Service Provider and henceforth). One or more IAT(s) are assigned for every dialup number of this. That is, the IAT group is assigned for every ISP. Therefore, the remote access (RAS is called henceforth) function which IAT holds is mounted for every ISP. When \*\*\*\*\* tends to connect with a certain ISP, it is necessary to turn an applicable dialup number. In relay or a mail arrival exchange system, IAT which has an RAS function translates this connected line identification, and connects it to IAT according to routing table. IAT is connected to the authentication server of ISP applicable with reference to the system data after a PPP (Point to Point Protocol) termination and in IAT. ISP assigns an IP address (IP:InternetProtocol) to \*\*\*\*\* after the end of attestation. When \*\*\*\*\* tends to connect with other ISP, \*\*\*\*\* turns another dialup number and receives a message in another IAT in relay or a mail arrival exchange system.

[0003]

[Problem(s) to be Solved by the Invention]Therefore, since IAT is divided and installed for every ISP, and also IAT is connected to the access router in an access point via LAN and it is connected to the router of ISP via WAN, it is necessary to prepare an access router for every ISP. That is, since sharing of IAT or RAS is not carried out in this way, it is a burden with big plant-and-equipment investment also for ISP also for the career, and there is a problem of not having led to reduction at the Internet access charge.

[0004]The purpose of this invention is to measure improvement in reduction of efficient employment of IAT, and plant-and-equipment investment, and member service by sharing one IAT between two or more providers.

[0005]

[Means for Solving the Problem]In order to attain the above-mentioned purpose, an Internet access method of this invention, In an Internet access method using an access server provided with the Internet access trunk which remote accesses an Internet Service Provider, Said Internet access trunk is characterized by having an accessing means which accesses two or more Internet Service Providers by a unified dialup number.

[0006]Said accessing means, It is characterized by discriminating said Internet access service provider from a user name (domain name) of \*\*\*\*\* and a password which have received an Internet Service Provider's service using a proxy server currently installed in an access point.

[0007]Said accessing means, It installs in an access point. It is characterized by discriminating an authentication server of an Internet Service Provider who checks user authentication from a user name (domain name) of \*\*\*\*\* and a password which have received an Internet Service Provider's service using a certain proxy server.

[0008]Said accessing means, An IP address of a router connected to said Internet Service Provider from system data which carried out internal organs to said proxy server, an IP address of an applicable Internet Service Provider's DNS server, and an IP address of \*\*\*\*\*. It is characterized by acquiring.

[0009]The 1st Internet accessing method of this invention, It is an Internet accessing method using an access server provided with the Internet access trunk which remote accesses an Internet Service Provider, Said Internet access trunk is characterized by accessing two or more Internet Service Providers by a unified dialup number.

[0010]The 2nd Internet accessing method of this invention, It is an Internet accessing method using an access server provided with the Internet access trunk which remote accesses an Internet Service Provider, A proxy server is used for said Internet access trunk, If an IP address of an authentication server which checks user authentication from a domain name to an authentication demand sent from \*\*\*\*\* is acquired, said authentication server is accessed, attestation is performed and attestation is successful, If an attestation Acknowledgement is replied to the aforementioned from subscriber terminal, and an IP address assignment request comes from said subscriber terminal after replying an attestation Acknowledgement to the aforementioned from subscriber terminal, An IP address assigned to a subscriber terminal and an IP address of an Internet Service Provider's DNS are acquired, and it is characterized by assigning said Internet Service Provider's IP address.

[0011]

[Embodiment of the Invention]Next, with reference to drawings, the embodiment of the Internet access system concerning this invention is described. Drawing 1 is shown and the member exchange system which has IAT to which this invention is applied PSTN network 101 (PHS:Plan Old Telephone Network), PHS network 102 (PHS:Personal Handy Phone System), ISDN network 103 (Integrated Service Digital Network), The relay exchange system 11 and the IAT module 12 (IAT:Internet AccessTrunk) which has two or more Internet access trunks (IAT) connected to the relay exchange system 11, HUB15 which is concentrating the output line (10BASE-T) from two or more IAT(s), The router 161,162 which processes routing (channel control), The proxy server 28 which is an access server, and the ISP1 provider 18 who offers service of the Internet, The ISP1 authentication server 181 of the ISP2 provider 19 who serves the Internet, and the ISP1 provider 18 who performs user authentication (check of a password etc.), The ISP2 authentication server 191 of the ISP2 provider 19 who performs user authentication (check of a password etc.), The relay data network 17 which connects the router 161,162, router 161, and ISP1 provider 18 and the ISP2 provider 19, It comprises the ISP1 terminal 131,132 a contract of is made with the ISP1 provider 18, and the ISP2 subscriber terminal 133 a contract of is made with the ISP2 provider 19.

[0012]In drawing 1, the access point contains the relay exchange system 11, the IAT module 12, HUB15, the router 161,162, and the proxy server 28. PSTN network 101 is a communications network which connects the ISP1 subscriber terminal 131 and the relay exchange system 11, PHS network 102 is a communications network which connects the ISP1 subscriber terminal 132 and the relay exchange system 11, and ISDN network 103 is a communications network which connects the ISP2 subscriber terminal 133 and the relay exchange system 11. Two or more subscriber terminals a contract of was made with two or more different ISP may be connected to each communications network. In drawing 1, on account of explanation, although it was considered as two sets, there may be more than it.

[0013]IATM12 comprises two or more IAT22, namely, comprises IAT22-1,22-2, ..., 22-n.

[0014]When the member who owns the ISP1 subscriber terminal 131 if drawing 1 is referred to dials a dialup number (telephone number of the common access point of the ISP1 provider 18 and the ISP2 provider 19), by the termination analysis of the relay exchange system 11. Although IAT22 to connect will be determined, if there is an empty channel which can connect then, it will connect with IAT22 equivalent to the channel. A message is received from two or more members in IAT22 [ vacant using the Marti hunting method (the dial-up number in this case is the pilot number with two or more circuits, and chooses one of two or more circuits) of an exchange system by the same dialup number ]. Even if it is further two or more providers, by assigning the same dialup number, a message is received in IAT22 [ vacant by the same number ]. Thus, saving or concentration of number resources can be aimed at by unifying a dialup number.

[0015]The PPP (Point to Point Protocol) termination of the call origination from a member's terminal is carried out to IAT22 through the modem which has carried out internal organs. Then, IAT22 connects office LAN to the proxy server 28 currently installed in the access point for attestation (check of the password entered from the member's terminal) of \*\*\*\*\* by course.

[0016]At this time, an authentication demand is performed with the proxy server 28 to ISP which recognizes corresponding ISP and corresponds. After completing attestation, the proxy server 28 acquires the IP address of \*\*\*\*\*, the IP address of the DNS server of ISP, and the IP address of an access router (router 161), and replies them to \*\*\*\*\*.

[0017]Reference of drawing 2 expresses the functional constitution figure of each IAT in IATM12. namely, the drawing 2 \*\*\*\* -- IAT22 comprises the modem 221 and the IAT control section 222 which operates by programmed control by the processor which is not illustrated. The IAT control section 222 comprises the PPP termination function part 223 and the IP address analyzer 224.

[0018]In drawing 2, the proxy server 28 comprises the server controlling part 281 which operates by programmed control by the processor which is not illustrated, and the storage parts store 282 which read-out and writing are made and stores system data. The storage parts store in this case may be a memory (for example, volatile memory, such as nonvolatile memory, such as a flash memory, and RAM), or may be recording media, such as a magnetic disk. System data including provider ID table 283, the data-address table 284, the attestation server address table 285, and two or more provider tables 286 are stored in the storage parts store 282. There is the provider table 286 for every provider, and in the provider table 286. The area of the default GW address table which stores the IP address (GW: gateway) of the default GW, It comprises area of the DNS address which stores the IP address of the DNS server (DNS:Distributed Name Service) of applicable ISP, and area of the member IP address pool which stores the IP address of the terminal of two or more \*\*\*\*\*.

[0019]Although some providers may have two or more sub-domains, In that case, area of a member IP address pool is consisted of by the provider table 286 for every area of a DNS address, and ISP for every ISP with the area of a default GW address table for every ISP.

[0020]The IAT control section 222 is provided with the transmission and reception circuit which is not illustrating for performing transmission and reception with the relay exchange system 11 through the modem 221, and the transmission and reception circuit which is not illustrating for performing transmission and reception with HUB15. The server controlling part 281 is provided with the transmission and reception circuit which is not illustrating for performing transmission and reception with the router 162.

[0021]Next, the outline of operation of this invention is explained with reference to drawing 2. The call origination from a member's terminal (an example ISP1 subscriber terminal or ISP2 subscriber terminal) is connected to the IAT control section 222 via the modem 221 which has carried out internal organs to IAT22. Connection with the IAT control section 222 from a subscriber terminal is made based on a PPP protocol. The PPP termination function part 223 of the IAT control section 222 performs processing based on a subscriber terminal and a PPP protocol. PPP (Point-to-Point Protocol) is specified by RFC1661 (RFC:Request for Comments), and is standardized by IETF (Internet Engineering TaskForce). Then, the IAT control section 222 is connected to the proxy server (going via HUB15 and the router 162) 28 via office LAN after the IP address analysis by the IP address analyzer 224. At this time, the server controlling part 281 of the proxy server 28 identifies ISP applicable from the user name (domain name) of ISP which \*\*\*\*\* makes a contract of. The server controlling part 281 recognizes the address of the authentication server of ISP (ISP1 provider or ISP2 provider) applicable from the attestation server address area of the provider table 286 stored in the storage parts store 282 from the user name (domain name) of ISP. Then, the server controlling part 281 sends out an authentication demand to applicable ISP, and performs attestation. After attestation is completed, the IAT control section 222 of IAT22 assigns the IP address of \*\*\*\*\* by communication with the proxy server 28.

[0022]The IAT control section 222 of IAT22 which acquired the \*\* side IP address, the IP address of a DNS server, and the IP address of the default GW from the proxy server 28 replies these data to \*\*\*\*\*, and a user packet transmission demand is urged to it. Then, the terminal of \*\*\*\*\* sends out a user packet by router 161 course from the IP address of the default GW.

[0023]Next, operation of an embodiment of the invention is explained with reference to drawing 1 -

drawing 6. Drawing 3 expresses the sequence of signal processing of IAT22. In order that \*\*\*\*\* a contract of is made with the ISP1 provider 18 may access the Internet via a provider now, Supposing it dials up using the ISP1 subscriber terminal 131, a call setup demand will receive a message in IAT22 of the IAT module 12 via PSTN network 101 and the relay exchange system 11. Then, the IAT control section 222 which received via the modem 221, Communication based on the ISP1 subscriber terminal 131 and a PPP protocol is performed, and the link (link setting 213 of drawing 2) by PPP is established the ISP1 subscriber terminal 131, IAT22, and in between (sequences 301-306 of drawing 3).

[0024]A PPP authentication demand (user ID and a password are added) is sent out from the ISP1 subscriber terminal 131 of \*\*\*\*\* after the termination of PPP from a member (sequence 306). The IAT control section 222 of IAT22 which received the authentication demand transmits the authentication demand packet (authentication demand 201 of drawing 2) of PPP which carried user ID and a password via the IP address part 224 to the proxy server 28 in an access point. In this case, the translation table stored in the storage parts store (it is in the IAT module 12) which is not illustrating the telephone number of the access point to which the IP address part 224 was applied from the ISP1 subscriber terminal 131 side (beforehand) the IP address corresponding for every access point telephone number is registered -- \*\*\*\* -- it uses and the IP address of the proxy server 28 is extracted. Using the extracted IP address, the IAT control section 222 will create an authentication demand packet, and will transmit to the proxy server 28.

[0025]Then, the server controlling part 281 of the proxy server 28 which received by HUB15 and router 162 course, The user name in the field of the authentication demand packet (authentication demand 201 of drawing 2) sent from IAT22 and the domain name of ISP are used, According to IP address search (after-mentioned) of the authentication server shown in drawing 4, the IP address (in this case, IP address of the ISP1 authentication server 181) of the authentication server of applicable ISP is read (sequence 318). The server controlling part 281 sends out an authentication demand packet (authentication demand 202 of drawing 2) to applicable ISP (ISP1 provider 18) according to the IP address of an authentication server (sequence 327).

[0026]The ISP1 provider 18 will hand an authentication demand packet to the ISP1 authentication server 181 which the ISP1 provider 18 has, if an authentication demand packet comes. The ISP1 authentication server 181 reads the user ID and the password in an authentication demand packet, Attestation of whether to be registered based on the user ID and password which were read by searching the user ID and the password which are registered into the database which is not illustrated for every user at the time of a contract is checked, The result is created as an authentication reply packet, and it replies to the proxy server 28 by ISP1 provider 18 course. the server controlling part 281 of the proxy server 28 after completing the attestation from the ISP1 provider 18 -- an authentication reply packet -- IAT22 -- sending a reply . The IAT control section 222 of IAT22 which received the authentication reply packet replies a PPP authentication response to the ISP1 subscriber terminal 131 (sequence 328,319,308).

[0027]Then, the ISP1 subscriber terminal 131 sends an IP address assignment request to IAT22 (sequence 309). If the IAT control section 222 of IAT22 receives an IP address quota demand, a quota request packet will be transmitted to the proxy server 28 (sequence 320).

[0028]Then, the server controlling part 281 of the proxy server 28, As shown in drawing 5, according to the structure (after-mentioned) of user-datum search, The IP address of the ISP1 subscriber terminal 131 of \*\*\*\*\* , the IP address of the DNS server of ISP, and the IP address of an access router are acquired, and it replies to the ISP1 subscriber terminal 131 of \*\*\*\*\* (sequence 329,321,310).

[0029]Next, if the control section 222 of IAT22 sends out the demand of an ISP fee collection start to the ISP1 provider 18, the ISP1 provider 18 will reply an ISP fee collection start response, and it will begin (sequence 322,323) to calculate the telex rate as use of the Internet.

[0030]On the other hand, the ISP1 subscriber terminal 131 which received the notice of IP address assignment will begin the Internet and communication via the ISP1 provider 18 (sequence 311). If a member terminates the communication to the Internet with the ISP1 subscriber terminal 131 and a circuit is cut soon, The link of the ISP1 subscriber terminal 131 and IAT22 is cut, the ISP1 provider's 18 accounting is completed, and suitcase hunt of IAT22 is canceled (sequences 312, 324, 325, 313,

and 314,316,317,315).

[0031]As mentioned above, although the case where the Internet was accessed from the ISP1 subscriber terminal 131 was explained, Also when the Internet is accessed from the ISP1 subscriber terminal 132, the point which communicates via PHS network 102 is different, but it cannot be overemphasized that operation of IAT22 and the proxy server 28 is the same. Also when the Internet is accessed from the ISP2 subscriber terminal 133, as the proxy server 28 was explanation of the above-mentioned operation, It cannot be overemphasized that the ISP2 provider 19 and the ISP2 authentication server 191 are chosen, and the ISP2 subscriber terminal 133 communicates with the Internet via the ISP2 provider 19.

[0032]Next, the structure of search of the address of the ISP authentication server of drawing 4 is explained. Provider ID, the table address, and the data address are stored in provider ID table 283 for every ISP, respectively. Although the table address shows the table address of the attestation server address table 285, the table address in provider ID table 283 currently assigned for every ISP is in common (the same table address). it is shown in the attestation server address table 285 for every ISP — each attestation server address storing is carried out. Provider ID is an index which identifies a provider. This is called for from a user name (domain name). Namely, the server controlling part 281 of the proxy server 28 of drawing 2, If an authentication demand packet is received, will extract a user name (domain name) from Program Data Unit (PDU) in the field of an authentication demand packet, and the user name decided beforehand will be made into an index, Provider ID, a table address, and a data address are acquired from provider ID table 283. And the server controlling part 281 accesses the attestation server address table 285 of the storage parts store 282 from the table address searched with provider ID table 283, An attestation server address is acquired by making into an index provider ID acquired on the provider table 283, and it asks for the IP address of an authentication server. Therefore, even if each provider's access point dialup number is common, it can distribute to the authentication server of the provider who connected.

[0033]Next, the structure of search of the user datum of drawing 5 is explained. First, the server controlling part 281 of the proxy server 28 of drawing 2, The data-address table 284 in the storage parts store 282 is subtracted from the data address for which it asked with provider ID table 283 of drawing 4, and the table address of the provider table 286 is acquired by making into an index provider ID calculated with provider ID table 283. Next, the server controlling part 281 pulls the provider table 286 which is in the storage parts store 282 by the table address acquired on this data-address table 284, A user's attribute (subdomain name in the field of an assignment request packet) decided beforehand is made into an index, The IP address of a member's terminal is acquired by searching a member IP address applicable from the user IP address pool which is a user datum, and the IP address of the default GW and the IP address of DNS are acquired.

[0034]Next, with reference to drawing 6, IAT explains the process flow to attestation and acquisition of each IP address using a proxy server. First, IAT22 makes provider ID introduce by transmitting an authentication demand packet to the proxy server 28, in order to discriminate the provider of ISP made into the purpose from the domain name in the field of an authentication demand packet (Step S601 of drawing 6). In a proxy server, the address of the authentication server of ISP applicable from provider ID is recognized (Step S602). In a proxy server, the authentication server of applicable ISP is accessed and attestation is performed (Step S603).

[0035]IAT22 will reply an operation confirming response (O.K.) to the terminal of \*\*\*\*\*, if a success of attestation is recognized by the authentication reply from a proxy server (Step S604, S606).

[0036]By transmitting an assignment request packet to the proxy server 28, if IAT22 receives an IP address quota demand from the terminal of \*\*\*\*\*, According to the structure of the user-datum search shown in drawing 5, the IP address of the terminal of \*\*\*\*\*, the IP address of the DNS server of ISP, and the IP address of an access router are acquired (Step S607, S608).

[0037]Thus, target ISP can be recognized not with a connected line identification but with the user name (domain name) and password of \*\*\*\*\*, and an user datum required for ISP connection can be acquired from a proxy server (Step S609).

[0038]

[Effect of the Invention]As explained above, the 1st effect of this invention is that plant-and-



equipment investment is reducible by sharing of IAT. The reason is because the number of equipment of IAT is reducible by sharing IAT between two or more providers. Therefore, since it is not necessary to prepare a yard LAN facility for every provider, cost is reducible. Since it is not necessary to prepare an access router for every provider, cost is reducible.

[0039]The 2nd effect is being able to perform improvement in member service. The reason is because the member can access the Internet, without being conscious of a provider. Therefore, even if it has joined two or more providers, it is connectable with an internet provider by one dialup number.

[0040]The 3rd effect is that a new business opportunity can be born to the career side. Since the reason is connectable with two or more providers from one IAT, the career side can provide two or more providers with the cheap Internet access business of cost. Therefore, since the provider side can also realize reduction of access servers, it becomes possible to entrust an Internet access function to the career side. Therefore, the career side can create new business and can raise a profit.

---

[Translation done.]



**\* NOTICES \***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

**DESCRIPTION OF DRAWINGS**

---

**[Brief Description of the Drawings]**

[Drawing 1]It is a system block figure showing the outline of the Internet access system using IAT of this invention.

[Drawing 2]It is a block diagram showing the composition of the function of IAT shown by drawing 1, and an Internet access system.

[Drawing 3]It is a sequence diagram showing the sequence of signal processing between the subscriber terminal of drawing 2, and an ISP provider.

[Drawing 4]In the proxy server of drawing 2, it is a schematic diagram showing the mechanism of searching the address of an authentication server.

[Drawing 5]In the proxy server of drawing 2, it is a schematic diagram showing the mechanism of searching an user datum.

[Drawing 6]IAT of drawing 2 is the flow chart which showed the flow of attestation and IP address processing using the proxy server.

**[Description of Notations]**

- 11 Relay exchange system
  - 12 IAT module
  - 15 HUB
  - 17 Relay data network
  - 18 ISP1 provider
  - 19 ISP2 provider
  - 22 IAT
  - 28 Proxy server
  - 101 PSTN network
  - 102 PHS network
  - 103 ISDN network
  - 131,132 ISP1 subscriber terminal
  - 133 ISP2 subscriber terminal
  - 161,162 Router
  - 181 ISP1 authentication server
  - 191 ISP2 authentication server
  - 221 Modem
  - 222 IAT control section
  - 223 PPP termination function part
  - 224 IP address analyzer
  - 281 Server controlling part
  - 282 Storage parts store
  - 283 Provider ID table
  - 284 Data-address table
  - 285 Attestation server address table
  - 286 Provider table
-

[Translation done.]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-237892

(P2001-237892A)

(43)公開日 平成13年8月31日(2001.8.31)

(51)Int.Cl.<sup>7</sup>

識別記号

F I

テーマコード(参考)

H 0 4 L 12/56

G 0 6 F 13/00

3 5 4 A 5 B 0 8 9

G 0 6 F 13/00

3 5 4

H 0 4 M 3/00

B 5 K 0 3 0

H 0 4 M 3/00

H 0 4 L 11/20

1 0 2 A 5 K 0 5 1

9 A 0 0 1

審査請求 有 請求項の数 6 O L (全 9 頁)

(21)出願番号

特願2000-49130(P2000-49130)

(22)出願日

平成12年2月25日(2000.2.25)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 中村 政和

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100082935

弁理士 京本 直樹 (外2名)

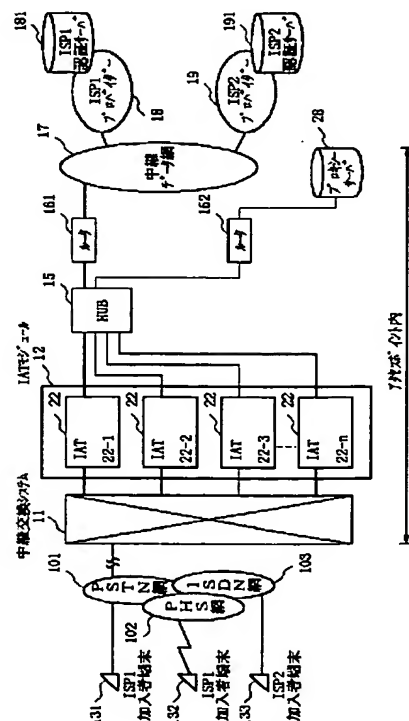
最終頁に続く

(54)【発明の名称】 アクセスサーバを用いたインターネットアクセス方式および方法

(57)【要約】

【課題】ダイアルアップインターネットアクセスを簡素化し、アクセスサーバを複数のプロバイダーで共有することによって設備投資を軽減する。

【解決手段】発加入者端末131からダイアルアップアクセス番号をダイヤルすると、中継交換システム11において、ダイアルアップアクセス番号を翻訳し、IAT22に着信する。PPP終端後、発加入者端末131のユーザ名(ドメイン名)とパスワードから該当するISPを認識し、該当ISPの認証サーバのアドレスを取得する。認証終了後、プロキシサーバ28に格納されている各ISPのユーザデータから発加入者端末のIPアドレス、アクセスルータのIPアドレス、DNSサーバのIPアドレスを取得し、当該ISPへアクセスを可能にする。このようにして1つのダイアルアップ番号で複数のプロバイダーにアクセスすることを可能にする。



## 【特許請求の範囲】

【請求項1】 インターネットサービスプロバイダーのリモートアクセスを行うインターネットアクセストラックを備えたアクセスサーバを用いたインターネットアクセス方式において、前記インターネットアクセストラックは、統一されたダイヤルアップ番号により複数のインターネットサービスプロバイダーにアクセスするアクセス手段を有することを特徴とするアクセスサーバを用いたインターネットアクセス方式。

【請求項2】 前記アクセス手段は、アクセスポイント内に設置してあるプロキシサーバを用いてインターネットサービスプロバイダーのサービスを受けている発加入者端末のユーザ名（ドメイン名）とパスワードとから前記インターネットアクセスサービスプロバイダーを識別することを特徴とする請求項1記載のアクセスサーバを用いたインターネットアクセス方式。

【請求項3】 前記アクセス手段は、アクセスポイント内に設置してあるプロキシサーバを用いてインターネットサービスプロバイダーのサービスを受けている発加入者端末のユーザ名（ドメイン名）とパスワードとからユーザ認証のチェックを行うインターネットサービスプロバイダーの認証サーバを識別することを特徴とする請求項1記載アクセスサーバを用いたインターネットアクセス方式。

【請求項4】 前記アクセス手段は、前記プロキシサーバに内蔵したシステムデータより前記インターネットサービスプロバイダーに接続するルータのIPアドレスと該当するインターネットサービスプロバイダーのDNSサーバーのIPアドレスと発加入者端末のIPアドレスとを取得することを特徴とする請求項1、2、または3記載のアクセスサーバを用いたインターネットアクセス方式。

【請求項5】 インターネットサービスプロバイダーのリモートアクセスを行うインターネットアクセストラックを備えたアクセスサーバを用いたインターネットアクセス方法であって、前記インターネットアクセストラックは、統一されたダイヤルアップ番号により複数のインターネットサービスプロバイダーにアクセスすることを特徴とするアクセスサーバを用いたインターネットアクセス方法。

【請求項6】 インターネットサービスプロバイダーのリモートアクセスを行うインターネットアクセストラックを備えたアクセスサーバを用いたインターネットアクセス方法であって、前記インターネットアクセストラックは、プロキシサーバを用いて、発加入者端末から発信される認証要求に対してドメイン名からユーザ認証のチェックを行う認証サーバのIPアドレスを取得し、前記認証サーバにアクセスして認証を実行させ、認証が成功すれば、認証確認応答を前記発加入者端末に返信し、認証確認応答を前記発加入者端末に返信後に前記加入者

端末からIPアドレス割当要求が来ると、加入者端末に割り当てるIPアドレスとインターネットサービスプロバイダーのDNSのIPアドレスとを取得し、前記インターネットサービスプロバイダーのIPアドレスを割り当てることを特徴とするアクセスサーバを用いたインターネットアクセス方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、インターネットアクセスシステムの方式および方法に関し、特に、インターネットアクセストラック（Internet Access Trunk：IATと呼ぶ）を有する中継交換または加入者交換システムのリモートアクセスサーバーの機能における共有アクセスサーバを用いたインターネットアクセス方式および方法に関する。

## 【0002】

【従来の技術】一般的に1つのISP（Internet Service Provider：インターネットサービスプロバイダー、以降、略してプロバイダーと呼ぶ場合もある）には1つまたは複数のダイヤルアップ番号が割り当てられている。このダイヤルアップ番号毎に1つまたは複数のIATが割り当てられている。つまり、IAT群はISP毎に割り当てられている。したがって、IATが保有するリモートアクセス（以降、RASと称す）機能は、ISP毎に実装されている。発加入者が、あるISPに接続しようとする時、該当するダイヤルアップ番号を回す必要がある。RAS機能を有するIATは、中継または着信交換システムにおいて、この着信番号を翻訳してルーティングテーブルに従いIATに接続する。IATは、PPP（Point to Point Protocol）終端後、IAT内のシステムデータを参照して該当するISPの認証サーバに接続する。さらに、認証終了後、ISPは発加入者に対してIPアドレス（IP：Internet Protocol）を割り振る。発加入者が他のISPに接続しようとする時には、発加入者は別のダイヤルアップ番号を回し、中継または着信交換システムにおいて別のIATに着信する。

## 【0003】

【発明が解決しようとする課題】従って、IATはISP毎に分割されて設置されており、更にIATはLAN経由でアクセスポイント内のアクセ斯拉ータに接続され、WAN経由でISPのルータに接続されているため、ISP毎にアクセ斯拉ータを用意する必要がある。すなわち、このようにIATまたはRASの共有がされていないため、キャリアにとってもISPにとっても設備投資が大きな負担となっており、インターネットアクセス料金に低減化につながっていないという問題点がある。

【0004】本発明の目的は、1つのIATを複数のプ

ロバイダで共有することによって IAT の効率的な運用、設備投資の削減及び加入者サービスの向上を計ることにある。

【0005】

【課題を解決するための手段】上記の目的を達成するために、本発明のインターネットアクセス方式は、インターネットサービスプロバイダーのリモートアクセスを行うインターネットアクセストラंकを備えたアクセスサーバを用いたインターネットアクセス方式において、前記インターネットアクセストラंकは、統一されたダイヤルアップ番号により複数のインターネットサービスプロバイダーにアクセスするアクセス手段を有することを特徴としている。

【0006】更に、前記アクセス手段は、アクセスポイント内に設置してあるプロキシサーバを用いてインターネットサービスプロバイダーのサービスを受けている発加入者端末のユーザ名（ドメイン名）とパスワードとから前記インターネットアクセスサービスプロバイダーを識別することを特徴としている。

【0007】更に、前記アクセス手段は、アクセスポイント内に設置してあるプロキシサーバを用いてインターネットサービスプロバイダーのサービスを受けている発加入者端末のユーザ名（ドメイン名）とパスワードとからユーザ認証のチェックを行うインターネットサービスプロバイダーの認証サーバを識別することを特徴としている。

【0008】更に、前記アクセス手段は、前記プロキシサーバに内蔵したシステムデータより前記インターネットサービスプロバイダーに接続するルータの IP アドレスと該当するインターネットサービスプロバイダーの DNS サーバの IP アドレスと発加入者端末の IP アドレスとを取得することを特徴としている。

【0009】また、本発明の第 1 のインターネットアクセス方法は、インターネットサービスプロバイダーのリモートアクセスを行うインターネットアクセストラंकを備えたアクセスサーバを用いたインターネットアクセス方法であって、前記インターネットアクセストラंकは、統一されたダイヤルアップ番号により複数のインターネットサービスプロバイダーにアクセスすることを特徴としている。

【0010】また、本発明の第 2 のインターネットアクセス方法は、インターネットサービスプロバイダーのリモートアクセスを行うインターネットアクセストラंकを備えたアクセスサーバを用いたインターネットアクセス方法であって、前記インターネットアクセストラंकは、プロキシサーバを用いて、発加入者端末から発信される認証要求に対してドメイン名からユーザ認証のチェックを行う認証サーバの IP アドレスを取得し、前記認証サーバにアクセスして認証を実行させ、認証が成功すれば、認証確認応答を前記発加入者端末に返信し、認

証確認応答を前記発加入者端末に返信後に前記加入者端末から IP アドレス割当要求が来ると、加入者端末に割り当てる IP アドレスとインターネットサービスプロバイダーの DNS の IP アドレスとを取得し、前記インターネットサービスプロバイダーの IP アドレスを割り当てることを特徴としている。

【0011】

【発明の実施の形態】次に、図面を参照して、本発明に係わるインターネットアクセスシステムの実施の形態を説明する。図 1 は、本発明が適用される IAT を有する加入者交換システムを示しており、PSTN 網 101

(PHS: Plan Old Telephone Network) と、PHS 網 102 (PHS: Personal Handy Phone System) と、ISDN 網 103 (Integrated Service Digital Network) と、中継交換システム 11 と、中継交換システム 11 に接続された複数のインターネットアクセストラंक (IAT) を有する IAT モジュール 12 (IAT: Internet Access Trunk) と、複数の IAT からの出力線 (10BASE-T) を集線している HUB 15 と、ルーティング (通信路制御) の処理を行うルータ 161、162 と、アクセスサーバであるプロキシサーバ 28 と、インターネットのサービスを行う ISP 1 プロバイダー 18 と、インターネットのサービスを行う ISP 2 プロバイダー 19 と、ユーザ認証 (パスワード等のチェック) を行う ISP 1 プロバイダー 18 の ISP 1 認証サーバ 181 と、ユーザ認証 (パスワード等のチェック) を行う ISP 2 プロバイダー 19 の ISP 2 認証サーバ 191 と、ルータ 161、162 と、ルータ 161 と ISP 1 プロバイダー 18 および ISP 2 プロバイダー 19 とを接続する中継データ網 17 と、ISP 1 プロバイダー 18 と契約している ISP 1 端末 131、132 と、ISP 2 プロバイダー 19 と契約している ISP 2 加入者端末 133 とから構成されている。

【0012】なお、図 1 において、アクセスポイントは、中継交換システム 11 と、IAT モジュール 12 と、HUB 15 と、ルータ 161、162 と、プロキシサーバ 28 とを含んでいる。また、PSTN 網 101 は ISP 1 加入者端末 131 と中継交換システム 11 とを接続する通信網であり、PHS 網 102 は ISP 1 加入者端末 132 と中継交換システム 11 とを接続する通信網であり、ISDN 網 103 は、ISP 2 加入者端末 133 と中継交換システム 11 とを接続する通信網である。また、それぞれの通信網には、複数の違った ISP と契約した複数の加入者端末が接続されても良い。また、図 1 では、説明の都合上、2 台としたが、それ以上であっても良い。

【0013】IATM 12 は、複数の IAT 22 で構成され、すなわち、IAT 22-1、22-2、・・・、

22-nから構成される。

【0014】図1を参照すると、ISP1加入者端末131を所有している加入者がダイヤルアップ番号（ISP1プロバイダー18とISP2プロバイダー19の共通のアクセスポイントの電話番号）をダイヤルすると中継交換システム11の着信分析によって、接続するIAT22を決定することになるが、そのとき接続可能な空きチャンネルがあればそのチャンネルに相当するIAT22に接続する。また、複数の加入者から同一ダイヤルアップ番号で、交換システムのマルチハンティング方式（この場合のダイヤルアップ番号は複数の回線を持つ代表番号であり、複数の回線の内の1つを選ぶ）を用いて空いているIAT22に着信する。さらに複数のプロバイダーであっても同一のダイヤルアップ番号を割り当てることによって、同一番号で空いているIAT22に着信する。このように、ダイヤルアップ番号を統一することにより番号資源の節約または集約を図る事ができる。

【0015】加入者の端末からの発呼は、IAT22に内臓してあるモデムを経てPPP（Point to Point Protocol）終端する。その後、IAT22は発加入者の認証（加入者の端末から入力されたパスワードのチェック）のために、アクセスポイント内に設置してあるプロキシサーバ28に局内LANを経由で接続する。

【0016】この時プロキシサーバ28では、対応するISPを認識し該当するISPに対して認証要求を行なう。認証が終了後、プロキシサーバ28は発加入者のIPアドレス、ISPのDNSサーバのIPアドレス、アクセスルータ（ルータ161）のIPアドレスを取得し発加入者へ返信する。

【0017】図2を参照すると、IATM12内の各IATの機能構成図を表している。すなわち、図2において、IAT22は、モデム221と、図示していないプロセッサによりプログラム制御で動作するIAT制御部222とから構成される。IAT制御部222は、PPP終端機能部223と、IPアドレス分析部224とから構成される。

【0018】更に、図2において、プロキシサーバ28は、図示していないプロセッサによりプログラム制御で動作するサーバ制御部281と、読み出しおよび書き込みができシステムデータを格納する記憶部282とから構成される。この場合の記憶部は、メモリ（例えば、フラッシュメモリ等の不揮発性メモリ、RAM等の揮発性メモリ）であっても、または磁気ディスク等の記録媒体であっても良い。記憶部282には、プロバイダーIDテーブル283と、データアドレステーブル284と、認証サーバアドレステーブル285と、複数のプロバイダーテーブル286とを含むシステムデータを格納している。プロバイダーテーブル286は、プロバイダー毎にあり、プロバイダーテーブル286には、デフォ

ルトGWのIPアドレス（GW：ゲートウェイ）を格納しているデフォルトGWアドレステーブルのエリアと、該当するISPのDNSサーバ（DNS：Distributed Name Service）のIPアドレスを格納しているDNSアドレスのエリアと、複数の発加入者の端末のIPアドレスを格納する加入者IPアドレスプールのエリアとから構成される。

【0019】なお、プロバイダーによっては、複数のサブドメインを持つ場合もあるが、その場合は、プロバイダーテーブル286には、ISP毎にデフォルトGWアドレステーブルのエリアと、ISP毎にDNSアドレスのエリアと、ISP毎に加入者IPアドレスプールのエリアとから構成される。

【0020】なお、IAT制御部222は、モデム221を介しての中継交換システム11との送受信を行うための図示していない送受信回路と、HUB15との送受信を行うための図示していない送受信回路を備えている。また、サーバ制御部281は、ルータ162との送受信を行うための図示していない送受信回路を備えている。

【0021】次に、図2を参照して、本発明の動作の概略を説明する。加入者の端末（例では、ISP1加入者端末またはISP2加入者端末）からの発呼は、IAT22に内臓してあるモデム221を経由してIAT制御部222に接続される。加入者端末からIAT制御部222への接続は、PPPプロトコルに基づいて行われる。IAT制御部222のPPP終端機能部223が加入者端末とPPPプロトコルに基づいた処理を行う。なお、PPP（Point-to-Point Protocol）は、RFC1661（RFC：Request for Comments）によって規定され、IETF（Internet Engineering Task Force）によって標準化されている。その後、IAT制御部222は、IPアドレス分析部224によるIPアドレス分析後、局内LANを経由して（HUB15およびルータ162を経由して）プロキシサーバ28に接続する。この時、プロキシサーバ28のサーバ制御部281は、発加入者の契約するISPのユーザ名（ドメイン名）から該当するISPを識別する。更に、サーバ制御部281は、ISPのユーザ名（ドメイン名）から記憶部282に格納されているプロバイダーテーブル286の認証サーバアドレスエリアから該当するISP（ISP1プロバイダーまたはISP2プロバイダー）の認証サーバのアドレスを認識する。その後、サーバ制御部281は、該当するISPに対して認証要求を送出し認証を実行する。認証が完了したのちIAT22のIAT制御部222は、発加入者端末のIPアドレスをプロキシサーバ28との通信により割り当てる。

【0022】発側IPアドレス、DNSサーバのIPア

ドレス、およびデフォルトGWのIPアドレスをプロキシサーバ28から取得したIAT22のIAT制御部222は、これらのデータを発加入者に返信して、ユーザパケット送信要求を促す。すると、発加入者の端末は、デフォルトGWのIPアドレスよりルータ161経由でユーザパケットを送出する。

【0023】次に、図1～図6を参照して、本発明の実施の形態の動作について説明する。図3はIAT22での信号処理のシーケンスを表わしている。今、ISP1プロバイダ18と契約している発加入者がプロバイダ18経由でインターネットのアクセスを行うために、ISP1加入者端末131を使用してダイヤルアップしたとすると、呼設定要求がPSTN網101および中継交換システム11を経由して、IATモジュール12のIAT22に着信する。すると、モデム221を介して受信したIAT制御部222は、ISP1加入者端末131とPPPプロトコルに基づいた通信を行い、ISP1加入者端末131とIAT22と間でPPPによるリンク（図2のリンク設定213）が確立される（図3のシーケンス301～306）。

【0024】加入者からのPPPの終端後、発加入者のISP1加入者端末131よりPPP認証要求（ユーザIDおよびパスワードを付加）が送出される（シーケンス306）。認証要求を受信したIAT22のIAT制御部222は、IPアドレス部224を介してユーザIDおよびパスワードを載せたPPPの認証要求パケット（図2の認証要求201）をアクセスポイント内のプロキシサーバ28に送信する。この場合、IPアドレス部224は、ISP1加入者端末131側からかけたアクセスポイントの電話番号を図示していない記憶部（IATモジュール12内にある）に格納された変換テーブル（あらかじめ、アクセスポイント電話番号毎に対応したIPアドレスが登録されている）を用いて、プロキシサーバ28のIPアドレスを抽出する。その抽出したIPアドレスを用いて、IAT制御部222は、認証要求パケットを作成し、プロキシサーバ28宛に送信することになる。

【0025】すると、HUB15、ルータ162経由で受信したプロキシサーバ28のサーバ制御部281は、IAT22より送られてきた認証要求パケット（図2の認証要求201）のフィールド内にあるユーザ名およびISPのドメイン名を用いて、図4に示した認証サーバのIPアドレス検索（後述）に従って、該当するISPの認証サーバのIPアドレス（この場合、ISP1認証サーバ181のIPアドレス）を読み取る（シーケンス318）。更に、サーバ制御部281は、認証サーバのIPアドレスに従って、該当するISP（ISP1プロバイダ18）に認証要求パケット（図2の認証要求202）を送出する（シーケンス327）。

【0026】ISP1プロバイダ18は認証要求パケ

ットが来ると、ISP1プロバイダ18にあるISP1認証サーバ181に認証要求パケットを渡す。ISP1認証サーバ181は、認証要求パケット内にあるユーザIDおよびパスワードを読み取り、その読み取ったユーザIDおよびパスワードを基に、図示していないデータベースに契約時に各ユーザ毎に登録されているユーザIDおよびパスワードを検索することにより登録されているかどうかの認証のチェックを行い、その結果を認証応答パケットとして作成し、ISP1プロバイダ18経由でプロキシサーバ28に返信する。ISP1プロバイダ18からの認証が終了後、プロキシサーバ28のサーバ制御部281は、認証応答パケットをIAT22の返信する。認証応答パケットを受信したIAT22のIAT制御部222は、ISP1加入者端末131にPPP認証応答を返信する（シーケンス328、319、308）。

【0027】すると、ISP1加入者端末131は、IPアドレス割当要求をIAT22に発信する（シーケンス309）。IAT22のIAT制御部222がIPアドレス割り当て要求を受信したならば、割り当て要求パケットをプロキシサーバ28に送信する（シーケンス320）。

【0028】すると、プロキシサーバ28のサーバ制御部281は、図5に示したように、ユーザデータ検索の仕組み（後述）に従って、発加入者のISP1加入者端末131のIPアドレス、ISPのDNSサーバのIPアドレス、およびアクセスルータのIPアドレスを取得し、発加入者のISP1加入者端末131に返信する（シーケンス329、321、310）。

【0029】次に、IAT22の制御部222はISP課金開始の要求をISP1プロバイダ18に送出すると、ISP1プロバイダ18はISP課金開始応答を返信すると共にインターネットの使用としての通信料を計算し始める（シーケンス322、323）。

【0030】一方、IPアドレス割当の通知を受けたISP1加入者端末131は、ISP1プロバイダ18を経由してインターネットと通信を始めることになる（シーケンス311）。やがて、加入者がISP1加入者端末131でインターネットへの通信を終了させ、回線を切断すると、ISP1加入者端末131とIAT22とのリンクが切断され、ISP1プロバイダ18の課金処理が終了し、IAT22のトランクハントが解除される（シーケンス312、324、325、313、314、316、317、315）。

【0031】以上、ISP1加入者端末131からインターネットをアクセスする場合について、説明したが、ISP1加入者端末132からインターネットをアクセスした場合も、PHS網102を介して通信を行う点は違うが、IAT22およびプロキシサーバ28の動作が同じであることは言うまでもない。また、ISP2加

10

20

30

40

50



入者端末133からインターネットをアクセスした場合も、プロキシサーバ28が、上記の動作の説明でしたように、ISP2プロバイダ19およびISP2認証サーバ191を選択し、ISP2加入者端末133がISP2プロバイダ19を介してインターネットと通信を行うことは言うまでもない。

【0032】次に、図4のISP認証サーバのアドレスの検索の仕組みについて説明する。プロバイダIDテーブル283には、ISP毎に、プロバイダIDと、テーブルアドレスと、データアドレスがそれぞれ格納されている。なお、テーブルアドレスは、認証サーバアドレステーブル285のテーブルアドレスを示しているが、プロバイダIDテーブル283内にあるISP毎に割り付けられているテーブルアドレスは共通（同一のテーブルアドレス）である。認証サーバアドレステーブル285には、ISP毎にある各認証サーバアドレス格納されている。プロバイダIDは、プロバイダを識別するインデックスである。これは、ユーザ名（ドメイン名）より求められる。すなわち、図2のプロキシサーバ28のサーバ制御部281は、認証要求パケットを受信すると、ユーザ名（ドメイン名）を認証要求パケットのフィールド内にあるProgram Data Unit（PDU）から抽出し、あらかじめ決められているユーザ名をインデックスとして、プロバイダIDテーブル283からプロバイダIDとテーブルアドレスとデータアドレスとを取得する。そして、サーバ制御部281は、プロバイダIDテーブル283で検索したテーブルアドレスから記憶部282の認証サーバアドレステーブル285をアクセスし、プロバイダIDテーブル283で取得したプロバイダIDをインデックスとして、認証サーバアドレスを取得し、認証サーバのIPアドレスを求める。従って、各プロバイダのアクセスポイントダイヤルアップ番号が共通でも、接続したプロバイダの認証サーバに振り分けることができる。

【0033】次に、図5のユーザデータの検索の仕組みについて説明する。まず、図2のプロキシサーバ28のサーバ制御部281は、図4のプロバイダIDテーブル283で求めたデータアドレスから記憶部282にあるデータアドレステーブル284をひき、プロバイダIDテーブル283で求めたプロバイダIDをインデックスとしてプロバイダテーブル286のテーブルアドレスを取得する。次にサーバ制御部281は、このデータアドレステーブル284で取得したテーブルアドレスにより記憶部282にあるプロバイダテーブル286をひき、あらかじめ決められているユーザの属性（割当要求パケットのフィールド内にあるサブドメイン名）をインデックスとして、ユーザデータであるユーザIPアドレスプールから該当する加入者IPアドレスを検索することで加入者の端末のIPアドレスを取得すると共に、デフォルトGWのIPアドレスと、DNSのIPア

ドレスを取得する。

【0034】次に、図6を参照して、IATがプロキシサーバを用いて、認証および各IPアドレスの取得までの処理フローについて説明する。まず、IAT22は、プロキシサーバ28に対し、認証要求パケットを送信することにより、認証要求パケットのフィールドにあるドメイン名から目的とするISPのプロバイダを識別するためにプロバイダIDを導入させる（図6のステップS601）。プロキシサーバでは、プロバイダIDから該当するISPの認証サーバのアドレスを認識する（ステップS602）。更に、プロキシサーバでは、該当するISPの認証サーバにアクセスし、認証を実行する（ステップS603）。

【0035】IAT22は、プロキシサーバからの認証応答により認証の成功を認識すると、発加入者の端末に動作確認応答（OK）を返信する（ステップS604、S606）。

【0036】更に、IAT22は、発加入者の端末からIPアドレス割り当て要求を受信すると、プロキシサーバ28に対し、割当要求パケットを送信することにより、図5に示したユーザデータ検索の仕組みに従って発加入者の端末のIPアドレス、ISPのDNSサーバのIPアドレス、およびアクセスルータのIPアドレスを取得する（ステップS607、S608）。

【0037】このように、着信番号ではなく発加入者のユーザ名（ドメイン名）とパスワードで目的のISPを認識し、ISP接続に必要なユーザデータをプロキシサーバから取得することができる（ステップS609）。

【0038】

【発明の効果】以上説明したように、本発明の第1の効果は、IATの共有化により設備投資が削減できることである。その理由は、IATを複数のプロバイダで共有することによりIATの設備数を削減できるためである。そのため、プロバイダ毎に構内LAN設備を用意する必要がないのでコストを削減することができる。また、プロバイダ毎にアクセスルータを用意する必要がないのでコストを削減することができる。

【0039】第2の効果は、加入者サービスの向上ができることである。その理由は、加入者はプロバイダを意識することなしにインターネットにアクセスできるためである。そのため、複数のプロバイダに加入していても1つのダイヤルアップ番号でインターネットプロバイダに接続できる。

【0040】第3の効果は、キャリア側に新たなビジネスチャンスが生まれることができることである。その理由は、1つのIATから複数のプロバイダに接続できることから、キャリア側が複数のプロバイダにコストの安いインターネットアクセスビジネスを提供できる。そのため、プロバイダ側もアクセスサーバーの削減を

11

12

実現することができるので、インターネットアクセス機能をキャリア側に委託することが可能となる。従って、キャリア側は新たなビジネスを創造し収益を上げることができる。

#### 【図面の簡単な説明】

【図1】本発明のIATを用いたインターネットアクセスシステムの概要を示したシステムブロック図である。

【図2】図1で示したIATおよびインターネットアクセスシステムの機能の構成を示したブロック図である。

【図3】図2の加入者端末とISPプロバイダーとの間の信号処理のシーケンスを示したシーケンス図である。

【図4】図2のプロキシサーバにおいて、認証サーバのアドレスを検索する仕組みを示した概略図である。

【図5】図2のプロキシサーバにおいて、ユーザデータを検索する仕組みを示した概略図である。

【図6】図2のIATがプロキシサーバを用いて、認証およびIPアドレス処理のフローを示したフローチャートである。

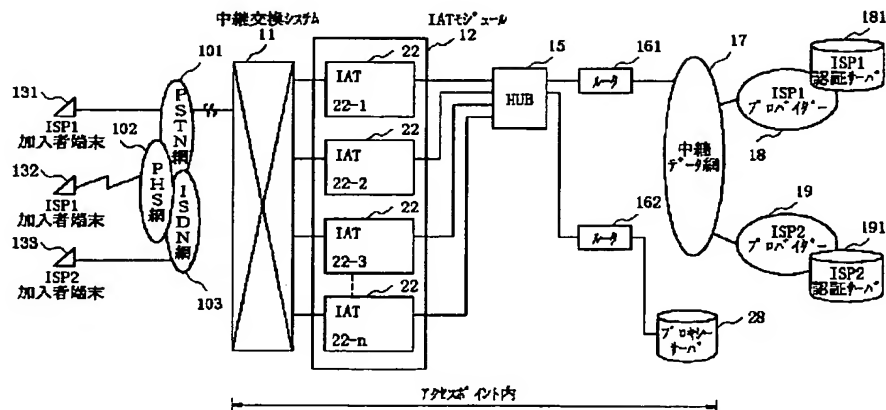
#### 【符号の説明】

- 11 中継交換システム  
12 IATモジュール  
15 HUB  
17 中継データ網

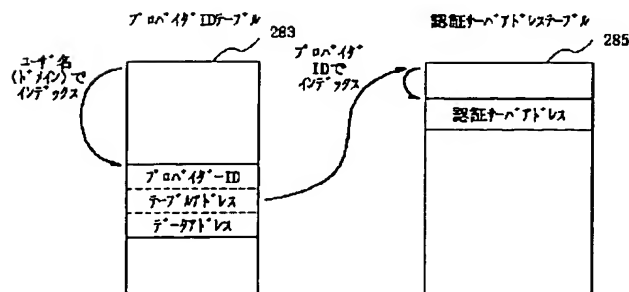
- \* 18 ISP1プロバイダー  
19 ISP2プロバイダー  
22 IAT  
28 プロキシサーバ  
101 PSTN網  
102 PHS網  
103 ISDN網  
131, 132 ISP1加入者端末  
133 ISP2加入者端末  
161, 162 ルータ  
181 ISP1認証サーバ  
191 ISP2認証サーバ  
221 モデム  
222 IAT制御部  
223 PPP終端機能部  
224 IPアドレス分析部  
281 サーバ制御部  
282 記憶部  
283 プロバイダIDテーブル  
284 データアドレステーブル  
285 認証サーバアドレステーブル  
286 プロバイダテーブル

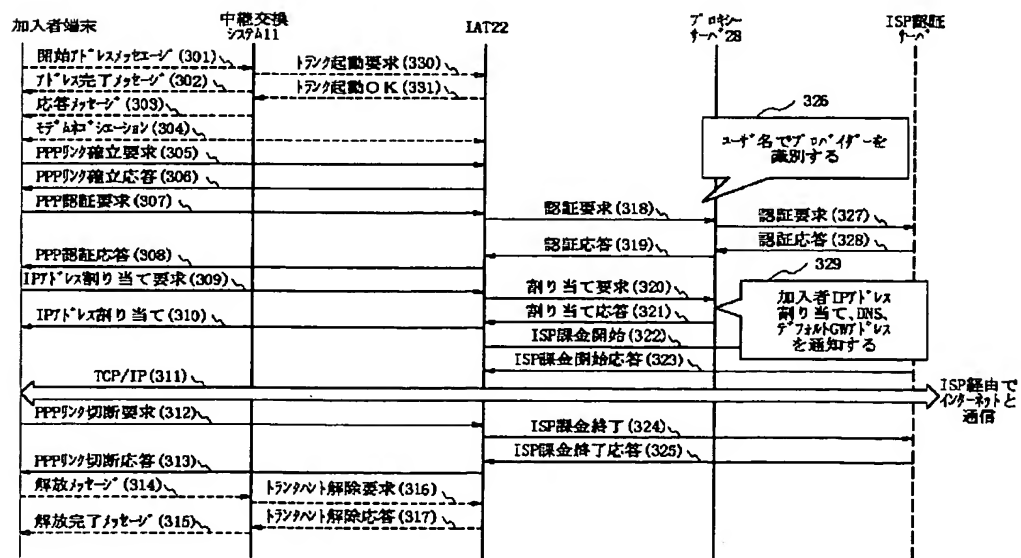
\*

【図1】

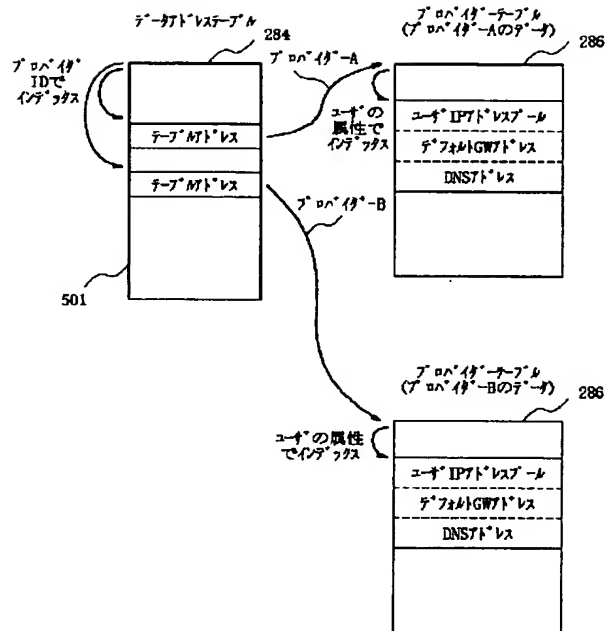


【図4】

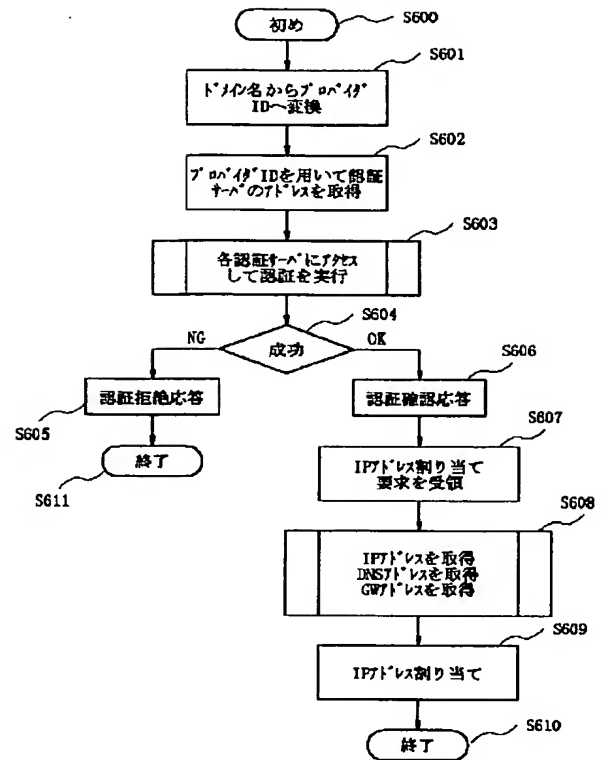




【図5】



【図6】



フロントページの続き

Fターム(参考) 5B089 GA11 GA19 GA31 HA10 HB03  
 JB14 KA11 KB06 KC58  
 5K030 GA05 HA08 HC01 HD03 HD09  
 JL07 JT03 KA05 KA16 LB02  
 5K051 AA05 BB02 DD00 GG02 HH17  
 JJ11  
 9A001 BB04 CC07 JJ25 JJ27 KK56